Temwork-4

problem statement

Using WIRESHARK observe the clata transferred in client server communicating using UDP & identity the UDP datagram

Objective

To observe the data transferred in client server communicooling using UDP + identity the UDP dutagram.

Theory Wireshark is a software fool used to monetor network Habbie through a network interface most widely used networking monttoning tool Viers: System administrators, network enginers, black . It has great UVI as well as convention (LI . It ofbers network monitoring on almost all types of network standards . et à free to we . It was steuted by Guald comber in 1997 Basic feautones of wireshark · Parlet Monitor - This sigment visually shows the packet flowing inside network The packets are shown with following information 1. source Address 2. Destination 3. Parket type 4. Hix dumps of Packets 5. Contents of packet in Tixt 6. Source Port 7. Destination Port.

working with wireshark · Import from capture tile: This feature lets you import packets dump from a tile to analyze turther. there are many formats supported by wirestark like peaping · Expost to capture file: whireshark lets you save the oresults as a capture file to continue working on them at later point of time. . Launch Wireshark: select an interface + click on bin icon to start capturing packets. · save the results as capture tile fexit after your done. UDP Analysis ling Wireshark Activity - Capture UPP traptic 1. Start a wireshak capture 2. open a command prompt 3. Type ipcontig/renew of press Enter to renew your DHCP assigned IP address. If youhove a static address this will not generate any UDP toolbic U. Type ipcontig/bushdas + press Enter to clear your Dr name cache 5 Type no lockup 2.8.88 fpress Enter to lookup the hostname bus IP addres 8.8.8.8

f. Close the command prompt

7. stop the wireshak capture.

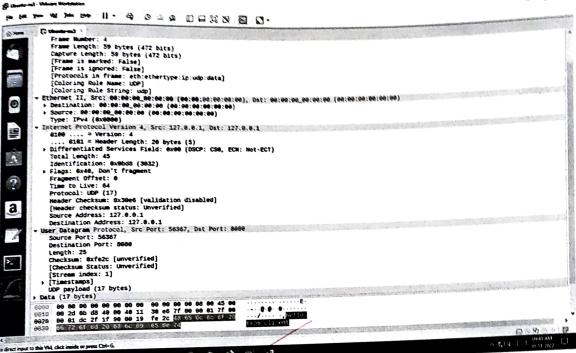
Term Work 4

Name: Vijay Anantpur

USN:2GI19CS176

Output:

Type have to se.



M

004

() Uhante na3 : 127.0.0.53 224.0,0.251 SSSS Mandard query 0x00000 FTR poppley ... \$355 0.000000000 8.007502176 3313 Standard Query Oxogoo PTR pophey - 3313 5353 Standard query 0-0000 PTR populary - 5353 24.017785640 45 644708785 8080 -60367 une: \$4147 - 8080 Lene 17 45.644817203 16367 -0000 000 - 56367 Lene 17 56.036498458 5353 Handard query 0x00000 PTR_pgpkey = 5353 is: Standard query 0x0 80.002470830 Mandard query Oxe4cs A connectivity check ubuntu.com OPT 46881 adard query 0xe4c5 A co Standard query 0x46d9 AAAA connectivity-check.ubunty.com OPT 53 80.002482315 44861 ndard query 0x46d9 AAAA 4888 Standard query response Ose4cS A connectivity check ubuntu com A 185.12.... 53 80.003936228 46881 Nandard query response 0x46d? AAAA connectivity check ubuntu com AAA... 53 80.004271600 179.103135229 46347 Standard query 0x44f7 A fixefox settings services mozilla com OPT DNS: Standard query 0x44f7 A firefox.se Standard query 0x8a0a AAAA firefox settings services mozilla.com OPT 53 179.103568537 46347 DNS: Standard query 0x8a0a AAAA firefo 179.104404941 46347 Mandard query response 0x4417 A fire ox settings services morals com A 34... 53 46347 Sendard query response Ostado AAAA firefox settings services mozilla.com.... 53 179.104441882 179.512694132 Standard guery 0x6eca A content signature 2.cdn mozilla net OPT 60743 60743 Standard query 0x06d9 AAAA content-signature-2 cdn.mozilla.net OPT 179.512945905 179.513484674 Standard query 0x547 c A content-signature-2, cdn.mozilla.net OPT 52355 DNS: Standard query 0x547c A conti 179.514091325 60743 Standard query response Oxocca A content signature 2 cdn mozilla net CNA.... 53 179.514187300 52355 Standard query response 0x547c A conjent-signature 2.cdn.mozilla.net CNA ... 53 se 0x547c A content-sig... 60743 Standard query response 0x06d9 AAAA content-signature-2.cdn.mozilla.net... 53 179,514313080 45431 Standard query Dx22fe A firefox-settings-attachments cdn.mozilla net OPT 53 181.005697700 dard query 0x22fe A firefor-settings-attac... 181.005949260 45431 Standard query 0x340b AAAA firefox settings attachments conmozilla.net 53 DNS: Standard query 0x340b AAAA firefox-settings-... 181.034522701 45431 Standard query response 0x22fe A firefox-settings-attachments.cdn.mozilla.... 53 DNS: Standard query response 0x22fe A firefox-setti... 181.035787256 45431 Standard query response 0x340b AAAA firefox-settings-attachments.cdn.m... 53 DNS: Standard query response 0x340b AAAA firefox-

DNS: Standard query 0xfbae A r3.o.lencr.org OPT

DNS: Standard query 0x37bc AAAA r3.o.lencr.org OPT

DOR 3 4 | D

ory

Standard query 0x/bap A r3.o.lencr.org OPT

Standard query 0x37bc AAAA r3.o.lencr.org OPT

181.104884464

181.105416124

to your computer, press Ctrl+Alt

39733

conclusion
Communicate observe the data transferred in client-server
the () De datagram
using wires hark tool
Learning outcomes
throng Outcomes
· Undustand the common allowed
· Undustand the significance of Inlineshould tool · Undustand how to analyze the UDP datagram owing
wirehark
Reberences
· https://www.wireshark.org
" W Richard Stevens, Bill Fenner, Andrew M Rodorf" "UNIX
Network Programming', Volume 1, Third telition, Praison 2004

Termwork-5

Problem statement

Using WIRESHARK analyse three way handshaking connection establishment, data transfer 4 connection termination in dieut-suru communication using TCP

Objective:

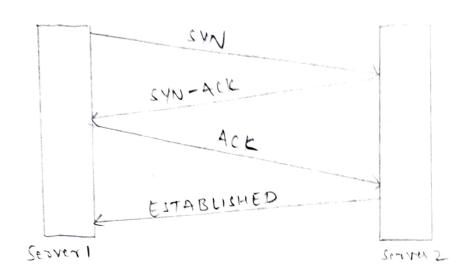
To analyze three way handshaking connection establishmen data transfer & connection termination in client-server communication using TCP

Theory Wireshark . It is a software tool used to monitor the network trabbic through a network interface · Most widely used network monitoring tool. · Users: system administers, network engineers, hetwork enthusiasts, network security projessionals · Et has great CIVI as well as a conventional CLI . It offer network monitoring on almost all types of network steindards · It is free to use · It was steeted by heald combez in 1997 Basic beautimes of wireshark · Packet Monitor - This segment trisually shows the parket flowing inside network The packets are shown with following information 1. source Address 2, Destination 3. Packet type 4. Hex dumps of Packets 5. Contents of parket is Text

6. source port

7. Destination port.

Three way Handshake



Norkins with wireshark.

Import from a capture file: This feature lets you import packets dump from a capture file to analyze further.

There are many townsts supported by winihark like opeapry.

Export to a capture file: Wireshark lets your form at results as a capture file to continue working on them at lase point of time. The supported formats are people

· Launch Wireshark, select an interpace of click on fin

· Save the result as a capture tile & exit after you are

TCP Analysis wing latereshark

i can to start capturing parkets.

· trom menuber, select capture -> options -> intufacer.

· In the interfaces chose a particular interface, note down
its IP, & click start button of selected adapter.

· This starts capturing packets.
· Buen the TCP surec & client programs to generate n/w
· Obsure the packets ACK, SYN, IYW-ACK listed on their

- source port: - This is port of host network wed for communicate

- Destination port: This the port of destination server.
- TCP sigment length: - It represents data length in siletted part

- selpelnu number: - It is a method wed by Wirehark to gine particular indering to each parket for tracking packets.
-Next sequence number: - It is sum of sequence number

4 the segment length of crement packet

Header length: It is length of Tep header 4 con vary from 20 to 60 · A major section of this TCP parket analysis is blag section of parket which gives further in-depth information about packet . The flag section has following parameters which are entisted with their respective significance · longestion latindow Reduced (CINR) . Et signals a decrease in transmission rate. -E(N-Echo: If is set on receiving earlier congestion notification - Vogent: It is set when the packet is to be considered a pronty. . At Cap wheelgement: It indicates whather church parket contains an acknowledgement packet or not · Push · The data should be saveed & removed from channel · Reset: It indicates on ellor in communication · SYN: Parket is Synchronized or NO + · FIN: tivalization - end of communication, subsection · biendow siere value: This is bufter size of cultint host · chetteum: It is used to verify that reviewed partet is OK or has an error. . chellesum status: - The parket checksum is not verified by défault but one can enable it by per requirements.

TermWork 5

Name:Vijay Anantpur USN:20119CS176

Output:

```
Willesheik Pastat is tabuhan tu
                          · frame id: 7d bytes on alle (507 bills), 7d bytes confluent (509 bills) on interface to, 1d o
                                            Interface 4d a 15.4
En apealation types (thermet (i)
Altival (these this path), per da thing afginage (e)
(time shift for this path), a disposage accounts
(froch time theory), a correspond occurred.
(The distinction previous captured from the house has been deft
(fine distinction previous captured from the house has been deft
(fine distinction of the correspond type).

Lines there extremely a track from the house has been deft
(fine distinction of the correspond type).
                                         [fine share extremite of trest firem of the firemit to firemit the firemit for the firemit to firemit for share firemit for the firemit firemit for the firemit firemit for firemit fire
                 [Coloring Rate name | Coloring | Coloring | Coloring Rate string: top.flags | Coloring Rate string: top.flags | Sayax | Coloring | C
                             > Destimition. An edical Robbs An (00:00:00:00:00:00:00)
                             ) Somice: Ba:ពុល:na ba-aalga (មុគ:គម្ងះគម្ងះគម្ងះមុខ)
                                        Type: 1PV4 (0x0000)
               * Internet Protocol Version 4, Src: 12/.0.0.1, Del: 127.0.0.1
                                       0100 ... = Version d
                                                          . 0101 = Header Length: 29 hytem (5)
                          . Differentiated Services Flein: 0x08 (DSGF) 650, EGH: Nat-EGI)
                                       total Length: 60
                                       Identification: 0x0000 (0)
                          * Flags: 0x40, Dun't fragment
                                               Fragment Offsett 9
                                  Time to Live: 64
                                  Protocol: ICP (6)
                                 Hember Checksonii bzacha (volidation disabled)
M Close
```

And the contract of	127.0.0,1	low - Loopback: lo	California in the Art
Lime		Comment	
21.741126789 21.741135191	4444 -43542		Seq = 0 Seq = 0 Ack = 1
1 741141807	44.03 -43542		Seq = 1 Ack = 1
£ 203907509	4444 - 43542 33542 - 4444		Seq = 1 Ack = 1
5.203932010 9.723730483	33542 4444	Lines Add	Seq = 1 Ack = 1025 Seq = 1 Ack = 1025
9.723740834	4444 -03542		Seq = 1025 Ack = 1025
Je. 7 items			T.
imit to display filter	Flow type: TCP	Flows	Addresses: Any
Help		Reset Diagram	¥ Close Save As

```
Wireshork - Packet 114 - Loopback: Lo
         Frame 114: 60 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface lo, id 0
              , Interface 1d: 0 (10)
                    Encapsulation type: Ethernet (1)
Arrival Time: Nov 10, 2022 10:22:00.388207120 IST
                   Artival time: not as as as a 22.00, 30020/170 IST [Time shift for this packet: 0.000000000 seconds] Epoch Time: 10005/4320.388207120 seconds [Time delta from previous captured frame: 3.056453415 seconds]
                  [Time delta from previous displayed frame: 3.050453415 seconds]
[Time delta from previous displayed frame: 3.050453415 seconds]
[Time since reference or first frame: 432.157094712 seconds]
Frame Number: 114
                 Frame Length: 66 bytes (528 bits)
Capture Length: 60 bytes (528 bits)
[Frame is marked: False]
                  [Frame is ignored: False]
 Frame 1s ignored False;
[protocols in frame: eth:ethertype:ip:tcp]
[coloring Rule Anne: 1CP SYM/FIN]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin == 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin = 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags.fin = 1]
[coloring Rule String: tcp.flags 8 0x02 || tcp.flags
         . Destination: 00.00:00 60:00:00 (00:00:00:00:00:00)
         Source: 00:00:00 (00:00:00 (00:00:00:00:00:00)
Type: 1Pv4 (0x0600)
v Internet Protocol Version 4, Src: 127.0.01, Ost: 127.0.0.1
      0100 .... = Version 4 .... 0101 = Header Length: 2a bytes (5) + Differentiated Service, Floor: 0x00 (OSCP: CSO, ECN: Not-ECT)
             Total Length: 52
             Identification: Walb38 (0908)
     Flags: 0x40, Don't fragment

6..., - Accerved bit: Not set

.1.... = Don't fragment: Set

.3... = More fragments: Not set
          Fragment Offset: 0
         Time to Live: 64
Protocol: FCP (6)
         Header Checksom: 0x218a [validation disabled]
                                                                                                                                                                                                                                                                                                                                                X Close
```

20/1/2

Concluin

we could analyze three way handshoking connection establishment data toansbest connection teremination in client -screen commencenceation using TCP.

Learning outcomes

eviderstand the significance of wireshark tool.

Understand how to analyze the TCP parkets using believe hark

References

w. Richard Stevens. Bill Former Andr. M. Rodol

W. Richard Stevens, Rill Fenner, Andrew. M. Rodorff: "UNIX Vetwork Programming", Volume 1, Third Edition Pearson 2004.